



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/665,040	09/19/2000	Jean-Francois Le Pennec	FR919990117	5465

7590 05/06/2004
Harry F Smith Esq
Ohlandt Greeley Ruggiero & Perle LLP
One Landmark Square
Stamford, CT 06901

EXAMINER

MCARDLE, JOSEPH M

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/06/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Sl

Office Action Summary

Application No.

09/665,040

Applicant(s)

LE PENNEC ET AL.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 September 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 9/19/2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2-4</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 5-9, 11-12, 14-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The examiner notes each of the aforementioned claims contains reference numbers pertaining to the drawings. It is unclear whether the reference numbers contained in the claims are intended to specifically limit the claim or provide a general reference for illustration purposes.
3. Claims 2, 3, and 13 are rejected under 35 U.S.C. 112, second paragraph, as being dependant on a rejected base claim.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 3, 6, 8 -13, 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu in view of Atkinson (U.S. Patent No. 5892904). In regards to claims 1, 9, and 10, Narasimhalu discloses a design that pertains to a method of verifying and validating the trustworthiness (guarantee it is virus-free, see

Art Unit: 2132

column 5, line 21) of data objects (i.e. files). Narasimhalu further discloses in column 4, lines 47-50 that a request for a certificate for an object is made by an information provider to a certification authority. This disclosure meets the first limitation set forth under claims 1, 9 and 10, which call for receiving a virus-free certificate request for a file from a system. Narasimhalu then goes on to disclose in column 5, lines 21-25 that the certifying authority is responsible for certifying objects meeting the defined trust criteria (i.e. is the object/file virus-free). This disclosure meets the limitations set forth under claims 1, 9 and 10, which call for determining whether the file is virus-free and certifying that the file is virus-free by issuing a certificate. Narasimhalu finally discloses in column 6, lines 35-41 that in response to receiving a certificate request, the certifying authority generates and sends a certificate back to the requesting information provider. This disclosure meets the limitation set forth under claims 1, 9 and 10, which call for sending back, in response to the virus-free certificate request, a virus-free certificate. However, Narasimhalu makes no mention of allowing the virus-free certificate to contain a file signature. Atkinson teaches in column 1, lines 48-52 that wide-spread distribution of executable files over open networks are at an increased risk of contracting computer viruses or other malicious code. Atkinson then discloses in column 2, lines 34-43 that in order to transfer a file over a communications network with confidence the file is signed to form a file signature. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Atkinson's teachings and disclosures on creating a file signature into Narasimhalu's design in order to achieve a design that is

capable of allowing the virus-free certificate to contain a file signature for the purposes of further reducing the risk that files become corrupted during transit.

3. In regards to claim 3, Narasimhalu further discloses in column 6, lines 32-34 that the information provider prepares a certificate request for a given distribution package (i.e. a file or other object) and sends it to the certifying authority. This disclosure meets the limitations set forth under claim 3, which call for have the certificate request specify a file for which a virus-free certificate is requested.

4. In regards to claims 6 and 15, Narasimhalu discloses in column 7, lines 28-36 that the certificate (indicating that an object/file is trustworthy) generated by the certification authority consists of a certificate body and the certificate authority signature (which is validated using the certificate authority's public key). It is also disclosed in the aforementioned location that the certificate body contains information relating to the certificate authority's identity, a time stamp for determining the validity of the certificate and a copy of the information contained in the certificate request, which includes and indication of an object (i.e. file) the certificate is being requested for. This disclosure meets the limitations set forth under claims 6 and 15, which call for the certificate to comprise a file identification, a virus-free certificate authority identification, a certificate signature for authenticating the virus-free certificate and an indication of the virus-free certificate validity. However, Narasimhalu's design makes no mention of allowing the virus-free certificate to contain a public key for decrypting the file signature. Atkinson teaches in column 1, lines 48-52 that wide-spread distribution of executable files over open networks are at an increased risk of contracting computer viruses or other

malicious code. Atkinson then discloses in column 2, lines 58-60 that the signature with which the file is signed with is formed using a public-private key signature algorithm such as the RSA public key cipher, is well known in the art. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Atkinson's teachings on how using public key ciphers for generating signatures are well known in the art into Narasimhalu's design in order to achieve a design that is capable of allowing the virus-free certificate to contain a public key for use in decrypting the file signature.

5. In regards to claim 8, Narasimhalu's design disclosed above meets all of the aforementioned limitations set forth under claim 1. However, Narasimhalu's design makes no mention of hashing the file to generate a file digest and encrypting the file digest using a private key. Atkinson discloses a in column 1, lines 48-52 that wide-spread distribution of executable files over open networks are at an increased risk of contracting computer viruses or other malicious code. Atkinson then discloses in column 2, lines 53-60 a method of generating a file signature that involves determining a cryptographic hash or digest of the file, which is then protected with a public-private key signature algorithm. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Atkinson's teaching on the need for reducing the risk of contacting computer viruses for files transmitted over open networks along with Atkinson's disclosure of creating a cryptographic file digest in order to achieve a design that is capable of generating a file signature by hashing the file and forming a digest which would then be encrypted using a private key.

6. In regards to claims 11, 16 and 17, Narasimhalu discloses a design in column 2, lines 35-42 in which a certificate (for certifying the trustworthiness of an object) is generated for a particular distribution package (i.e. file). It is also disclosed in the aforementioned location that the certificate body contains the name of the distributor package (file), indicating the association with a particular data package (file). This disclosure meets the limitations set forth under claims 11, 16 and 17 that call for determining a file that the virus-free certificate is associated with. Narasimhalu further discloses in column 8, lines 18-22 and in figure 2 that a certificate signature is contained in the certificate and is used to authenticate the signature. This disclosure meets the exact limitations set forth under claims 11, 16 and 17 that call for authenticating the virus-free certificate through the use of a certificate signature. However, Narasimhalu's design makes no mention of authenticating the file by allowing the virus-free certificate to contain a file signature for verifying the files authenticity. Atkinson teaches in column 1, lines 48-52 that wide-spread distribution of executable files over open networks are at an increased risk of contracting computer viruses or other malicious code. Atkinson then discloses in column 2, lines 34-43 that in order to transfer a file over a communications network with confidence the file is signed to form a file signature. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Atkinson's teachings and disclosures on creating a file signature into Narasimhalu's design in order to achieve a design that is capable of allowing the virus-free certificate to contain a file signature for the purposes of further reducing the risk that files become corrupted during transit.

7. In regards to claim 12, Narasimhalu and Atkinson's design disclosed above meets all of the aforementioned limitations set forth under claim 11. The combination of Narasimhalu and Atkinson further disclose the limitations set forth under claim 12, which call for decrypting the file signature using a public key contained in the virus-free certificate, hashing the file to generate a file digest and comparing the file digest to the decrypted file signature. Atkinson discloses in column 2, lines 58-60 that the signature with which the file is signed with is formed using a public-private key pair signature algorithm such as the RSA public key cipher, is well known in the art. Atkinson further discloses in column 2, lines 53-60 a method of generating a file signature that involves determining a cryptographic hash or digest of the file, which is then protected with the aforementioned public-private key signature algorithm. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Atkinson's teachings and disclosures on the use of public keys and file signatures into the Narasimhalu-Atkinson combination in order to achieve a design that is capable of allowing a file signature to be decrypted with a public key and then compared with a file digest to ensure the integrity and authenticity of the file.

8. In regards to claim 13, Narasimhalu further discloses in figure 2 that once the certificate is generated it is then verified to determine its authenticity. This disclosure meets the exact limitations set forth under claim 13 that call for validating the virus-free certificate.

9. Claims 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu and Atkinson as applied to claim 1 above and in further view of the

"Virus Bulletin" publication. In regards to claim 2, Narasimhalu and Atkinson's design disclosed above meets all of the aforementioned limitations set forth under claim 1. However, Narasimhalu and Atkinson's design makes no mention of allowing the virus-free certificate request to contain a list of one or a plurality of anti-virus programs to execute on the file to determine whether the file is virus-free or not. The "Virus Bulletin" publication discloses on page 12, under the heading "using just one anti-virus product" that the advantages of using multiple virus scanners outweighs the consequences of insufficient protection and that there are obvious benefits of using more than one scanning product such as providing a finer net that most computer viruses would be unable to penetrate. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the teachings disclosed in the "Virus Bulletin" publication into Narasimhalu and Atkinson's design in order to achieve a design that is capable of allowing the virus-free certificate request to contain a list of one or a plurality of anti-virus programs to execute on a file for the purpose of providing a finer virus detection net.

10. In regards to claim 4, Narasimhalu and Atkinson's design disclosed above meets all of the aforementioned limitations set forth under claim 1. However, Narasimhalu and Atkinson's design makes no mention of executing one or a plurality of anti-virus programs for detecting viruses. The "Virus Bulletin" publication discloses on page 12, under the heading "using just one anti-virus product" that the advantages of using multiple virus scanners outweighs the consequences of insufficient protection and that there are obvious benefits of using more than one scanning product such as providing a

finer net that most computer viruses would be unable to penetrate. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the teachings disclosed in the "Virus Bulletin" publication into Narasimhalu and Atkinson's design in order to achieve a design that is capable of allowing one or a plurality of anti-virus programs to be executed.

11. In regards to claim 5, Narasimhalu and Atkinson's design disclosed above meets all of the aforementioned limitations set forth under claim 1. However, Narasimhalu and Atkinson's design makes no mention of allowing the virus-free certificate request to contain a list of one or a plurality of anti-virus programs that have been executed on the file to determine whether the file is virus-free or not. The "Virus Bulletin" publication discloses on page 12, under the heading "using just one anti-virus product" that the advantages of using multiple virus scanners outweighs the consequences of insufficient protection and that there are obvious benefits of using more than one scanning product such as providing a finer net that most computer viruses would be unable to penetrate. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the teachings disclosed in the "Virus Bulletin" publication into Narasimhalu and Atkinson's teachings in order to achieve a design that is capable of allowing the virus-free certificate request to contain a list of one or a plurality of anti-virus programs that have been executed on a file for the purpose of determining what anti-virus programs were used in order to provide a finer virus detection net.

Art Unit: 2132

12. Claims 7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu and Atkinson as applied to claim 1 above and in further view of Muftic (U.S. Patent No. 5745574). In regards to claim 7, Narasimhalu further discloses in column 6, lines 42-46 that the certificate can be stored in a database along with the package (i.e. file) that it certifies. This disclosure meets the limitations set forth under claim 7 that call for identifying the system where the file and associated virus-free certificate are stored. However, Narasimhalu and Atkinson's design makes no mention of downloading updates of the virus-free certificate. Muftic discloses a design that pertains to public key based secure communication systems involving the use of certificates. Muftic then goes on to disclose in column 7, lines 21-41 a method directed towards updating certificates. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Muftic's design related to updating certificates into Narasimhalu and Atkinson's design in order to achieve a design that is capable of allowing certificates to be updated for the purposes of ensuring that the certificates remain current as well as for obtaining valid certificates.

13. In regards to claim 14, Narasimhalu further discloses in column 8, lines 28-50 that a certificate is verified as valid only when it meets all of the checks. This disclosure meets the limitation set forth under claim 14 that calls for determining whether the virus-free certificate is valid or not. However, Narasimhalu's design makes no mention of requesting an updated certificate if the current certificate is not valid. Muftic discloses a design that pertains to public key based secure communication systems involving the use of certificates. Muftic then goes on to disclose in column 7, lines 21-41 a method

Art Unit: 2132

directed towards updating certificates. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Muftic's design related to updating certificates into Narasimhalu and Atkinson's design in order to achieve a design that is capable of allowing certificates to be updated for the purposes of ensuring that the certificates remain current as well as for obtaining valid certificates.


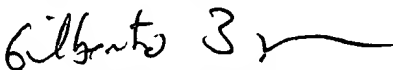
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jmm


Joseph McArdle
Examiner
Art Unit 2132

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100